ascertia

Enabling Adobe Reader to Trust other CA certificates

Trust is essential in today's e-business environment to meet legislative, regulatory and internal compliance requirements. Ascertia's products meet these needs by providing advanced digital signature trust services to confirm sign-off and approval within business documents and workflows, and confirm authenticity and integrity plus auditable traceability and accountability.

The PDF specifications are open and used by many different vendors to provide useful e-business solutions. With any unprotected PDF document, end-users are generally unable to determine if the document is fraudulent or genuine, who the originator was, whether the document is official, authorised or approved and has it been modified in any way. Many organisations would like to resolve such trust issues, have their PDF documents be accepted with confidence and to promote their brand image as secure and trustworthy.

The default configuration of the ubiquitous Adobe® Reader® products mean that any signatures that do not chain to the Adobe Root CA are shown with a status of "unknown". This document describes how other CA certificates can be added very simply as a new trust point within Adobe Reader. Now organisations can quickly add their own enterprise CAs or trust the Ascertia Root CA when reviewing SigningHub documents and find the right trust answer.

The Trust Symbols

When a document is signed by a trustworthy certificate issued by a Certificate Authority not chained to the Adobe Root CA, most end-users will not see a green 'trusted' tick, instead they see a blue question mark indicating the trust status is 'unknown'. The reason for this is that a certificate chain could not be built to an existing Trust Anchor. One of the easiest ways of getting your end-users to be able to trust your documents is to create a document like this that can present your Root CA certificate to Reader – now a green tick will be seen if the certificate is trusted. If the certificate is untrusted or if changes have been made to the document (invalidating the signature) then of course a red cross is shown. A Blue Rosette indicates a special "certify signed" document.

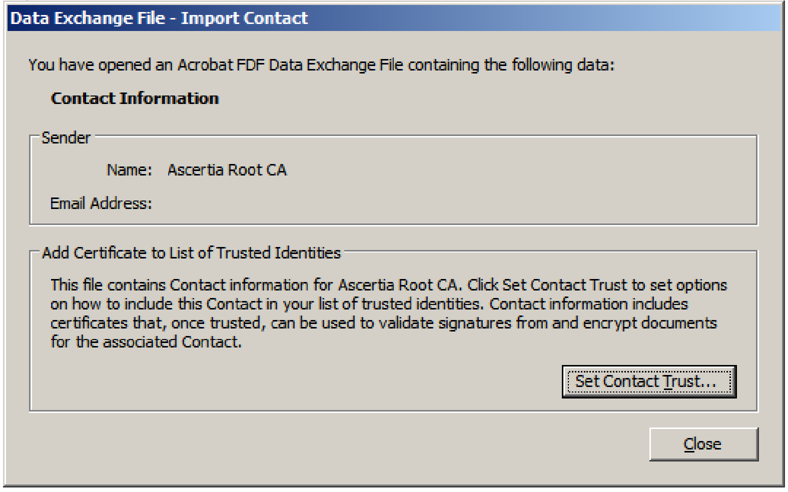
How to embed your Root Certificate

This PDF is an example of the type of document that can be created to add a new trust point to Reader. To the right is a digital signature signed by Rod Crook using and Ascertia CA chain. It is expected that everyone will see a blue question mark indicating that the signature has an unknown status. Follow these seven steps to get a tick:

Digitally Signed By: Rod Crook
Reason: I approve this document
2012/07/23 11:18:18 GMT +01:00
Rod Crook

Ascertia Limited
ascertia
Identity proven, Trust delivered

1) Click on the attachments tab on the left of the screen (it's a paperclip icon as shown):
2) Open the attachment "Ascertia Root CA Certificate.fdf" and this window is shown:


Data Exchange File - Import Contact

You have opened an Acrobat FDF Data Exchange File containing the following data:

Contact Information

Sender

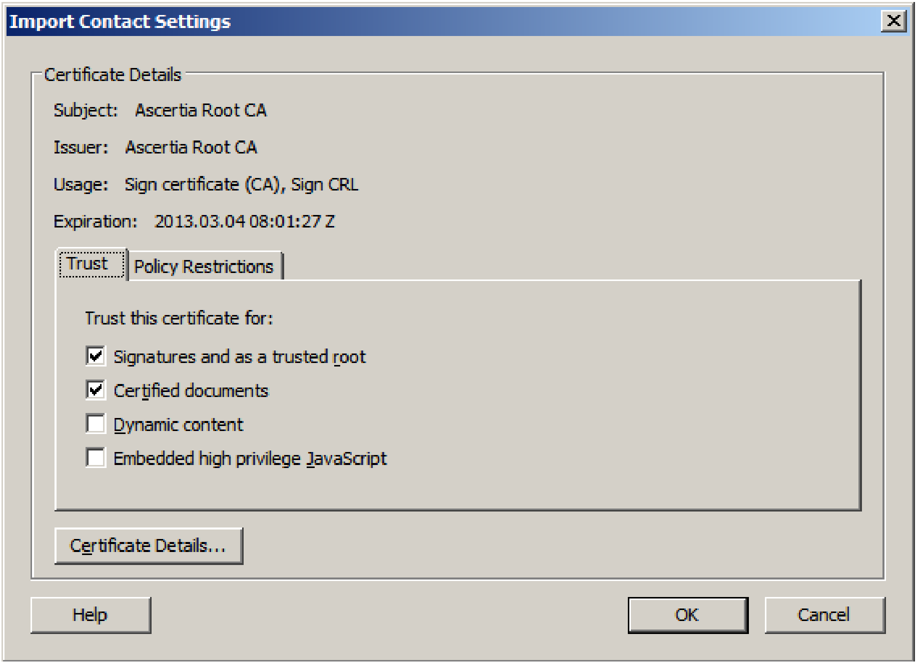
Name: Ascertia Root CA

Email Address:

Add Certificate to List of Trusted Identities

This file contains Contact information for Ascertia Root CA. Click Set Contact Trust to set options on how to include this Contact in your list of trusted identities. Contact information includes certificates that, once trusted, can be used to validate signatures from and encrypt documents for the associated Contact.

3) Click on the “Set Contact Trust “ button
4) This screen is now shown, now select the two check boxes as shown below:



Import Contact Settings

Certificate Details

Subject: Ascertia Root CA

Issuer: Ascertia Root CA

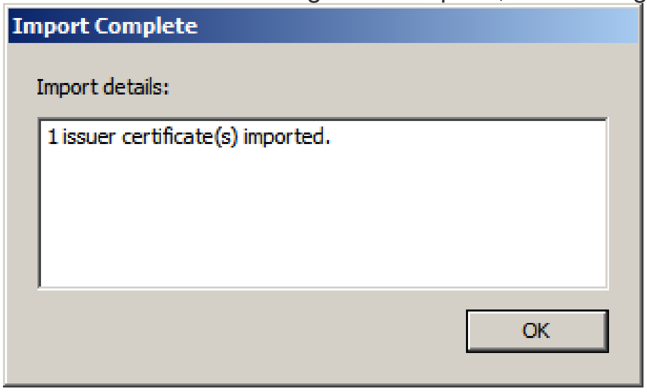
Usage: Sign certificate (CA), Sign CRL

Expiration: 2013.03.04 08:01:27 Z

Trust this certificate for:

☑ Signatures and as a trusted root
☑ Certified documents
☐ Dynamic content
☐ Embedded high privilege JavaScript

5) Click OK and the following window opens, click OK again



Import Complete

Import details:

1 issuer certificate(s) imported.

6) Now click the close button and the update to the Trusted Identities list is complete.
7) Now go back and click on the signature block shown on page 1 to re-validate it - you should see that the signature is now trusted with a blue rosette, indicating that this document is both signed and certified (locked against further unauthorized changes). If a certified signature is not used then a normal green tick would be shown.

If you need further help in understanding the trust aspects discussed here then contact Ascertia as shown below. The FDF files described can be easily created using Adobe® Acrobat®. The Ascertia products that can be used to sign and verify PDFs include Ascertia Docs, ADSS Signing Server and PDF Sign&Seal.

The Ascertia web-sites www.ascertia.com and www.SigningHub.com provide further details and also provide online demos or free trial use of these products.

For Sales support:	**Email sales@ascertia.com**
For Product support:	**Email support@ascertia.com**